Diese Website verwendet Cookies von Google, um Dienste anzubieten und den Traffic zu analysieren. Deine IP-Adresse und dein User-Agent werden zusammen mit Messwerten zur Leistung und Sicherheit für Google freigegeben. So können Nutzungsstatistiken generiert, Missbrauchsfälle erkannt und behoben und die Qualität des Dienstes gewährleistet werden.

WEITERE INFORMATIONEN OK

An unending variety of topics

Tuesday, August 28, 2007

Mutually private computation

From my article, The God Protocols:

> Imagine the ideal protocol. It would have the most trustworthy third party imaginable — a deity who is on everybody's side. All the parties would send their input to this god. God would reliably determine the results and return the output. In addition, God, being the ultimate in confessional discretion, would ensure that no party would learn anything more about the other party's input than they could learn from their own input and the output.
>
> Alas, in our temporal world we deal with humans rather than deities. Yet, too often we are forced to treat people in a nearly god-like manner because our infrastructure lacks the security needed to protect ourselves.

Pages

- Home

About Me

Nick Szabo

"A premier thinker about history, law and economics, and the lessons they have for security." -- Adam Shostack, Emergent Chaos

"Szabo comes out with these essays that leave me in awe." -- Brian Dunbar

"Reading material that is eclectic, challenging and endlessly fascinating." -- Sean McGrath, Propylon

"Like most blogs worth my attention, this blog is updated only infrequently. That is because the authors of blogs worth my attention only post when they have something to say that is true, relevant and not already known by their audience. Most of the human race does not have the skill to know when an idea has these three properties. The skill is particularly rare in the fields of politics and economics, which is why this blog is such a rare and valuable thing." -- Richard Hollerith

View my complete profile

To an astonishing extent, network security theorists have recently solved this problem. They have developed protocols that create virtual machines between two or more parties. Multi-party secure computation allows any number of parties to share a computation, each learning only what can be inferred from their own input and the output of the computation. These virtual machines have the exciting property that each party's input is held in strict confidence from the other parties. The program and the output are shared by the parties.

Blog Archive

- ► 2018 (1)
- ► 2017 (3)
- ► 2016 (4)
- ► 2015 (3)
- ► 2014 (3)
- ► 2013 (3)
- ► 2012 (8)
- ► 2011 (12)
- ► 2010 (9)
- ► 2009 (29)
- ► 2008 (55)
- ▼ 2007 (47)
  - ► December (1)
  - ► October (2)
  - ► September (8)
  - ▼ August (10)
    - Money and the problem of cooperation
    - Why the industrial revolution?
    - Mutually private computation

For example, we could run a spreadsheet across the Internet on this virtual computer. We would agree on a set of formulas and set up the virtual computer with these formulas. Each participant would have their own input cells, which remain blank on the other participants' computers. The participants share output cell(s). Each participant inputs their own private data into their input cells. Alice could only learn as much about the other participants' input cells as she could infer from her own inputs and outputs.

I go on to briefly describe applications such as confidential auditing and auctions with private bids, here.

Related articles: confidential auditing, secure time-stamping, advances in distributed security.

Some outside links to papers: secure time-stamping, multiparty secure computation.

Posted by Nick Szabo at 2:54 PM

Blind signatures

Personal jurisdiction before sovereignty

Smart contracts watch

Exit and freedom

Our new omniscient savior

Ten ways to make a political difference

Government for profit

► July (4)

► June (4)

► May (8)

► April (1)

► March (2)

► February (4)

► January (3)

► 2006 (130)

► 2005 (44)

Simple theme. Powered by Blogger.